REMARKS

This Submission is an amendment responsive to the above-identified final Office Action. Claims 14-16 have been canceled. Claims 17, 22, 27, 32, 37, 42, 47, 52, 57 and 62 have been amended to correct matters of form and to more particularly point out the subject matter of the invention, and no new matter has been added by this amendment. Accordingly, Claims 17-66 and 73-92 are now pending.

I. CLAIMS 17-66 AND 73-92 MEET THE REQUIREMENTS IN 35 U.S.C. § 112, ¶ ¶ 1 & 2

In the aforementioned Office Action, the Examiner indicates that claims 14-46 were rejected under 35 U.S.C. § 112, ¶ 1 as

> "containing subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention."

Such claims were further rejected under § 112, ¶ 1 as

> "containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the art that the inventor(s), at the time the application was filed, had possession of the claimed invention."

Moreover, claims 14 and 15 were rejected under § 112, ¶ 2 as

> "being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention.

As shown in the marked-up version at Exhibit A and as further explained below, the claim amendments obviate these rejections and render them moot. Applicants respectfully submit that all the pending claims meet the requirements set in 35 U.S.C. §112, and request withdrawal of these rejections.

A. The "Backwards" Compatible Term Has Been Deleted Thus Obviating the 35 USC § 112, ¶ 1 Rejection Based on Such Term

Claims 14, 15, 16, 22, 27, 32, 37 and 42 were rejected under § 112, ¶ 1 based on issues surrounding the term "backwards compatible with preexisting public key transformation schemes" (the "backwards compatible" term). Although this term is fully disclosed[1], and as disclosed it is correct, claims 14-16 have been canceled and claims 17, 22, 27, 32, 37, 42, 47, 52, 57 and 62 have been amended to remove this term such that the rejection is obviated. Accordingly, Applicants request that the § 112, ¶ 1 rejection based on the "backwards compatible" term be withdrawn.

B. Claims Reciting the "Acceleration" Term have been Canceled Thus Obviating the § 112, ¶ ¶ 1 and 2 Rejections Based on Such Term

The Examiner indicated a further rejection of Claims 14 and 15 under § 112, for reciting the term "step of decoding is accelerated" (the "acceleration" term). The examiner contends that the term is not disclosed nor enabled by the specification. Moreover, the examiner contends that the scope of the term is indefinite. However, the "acceleration term is fully disclosed[2], and as disclosed it meets the requirements of 35 U.S.C. § 112, ¶¶ 1 & 2, including written description, enablement and definiteness in scope.[3] Nonetheless, claims 14 and 15 have been canceled obviating the aforementioned rejection and rendering it inapplicable. Accordingly, the rejection should be reconsidered and withdrawan.

---

1 See, for example, Specification, pg. 10 ("A system encrypting data for another user performs the encryption process according to (3) [$C = M^e \bmod n$], independent of the number of factors of n." That is, M can be encrypted to form C by conventional encryption methods if n and e are known, and although decryption requires the factors of n, C can be decrypted even if C was formed by conventional encryption methods).

2 See, for example, Specification, pg. 7 ("perform encryption and decryption using a large (many digit) n much faster than heretofore possible."), and pgs. 9-10 ("encryption and decryption time can be substantially less than an RSA scheme using two primes;" "the encryption process can be accelerated;" "can be used to accelerate the process;" "can realize accelerated processing;" and "it is found that they [the sub-tasks M_1, M_2 and M_3] can most expeditiously be combined to a form of Chinese Remainder Theorem (CRT).").

3 The above recitations regarding the term "acceleration" (See, footnote 2) provide individually and collectively a standard for measuring the degree and scope of acceleration (e.g., faster than 2-prime RSA). Moreover, the specification as a whole gives meaning to the term acceleration. Accordingly, this term is clear and definite.

C. The Depenedent Claims Satisfy the Requirements of § 112, ¶ ¶ 1 and 2

As stated above, the rejections under 35 U.S.C. ¶ ¶ 1 and 2 are obviated by the claim amendments, and independent claims 17, 22, 27, 32, 37, 42, 47, 52, 57 and 62 meet all the requirements of 35 U.S.C. ¶ ¶ 1 and 2. Moreover, it is axiomatic that claims 17-66 and 73-92 that depend therefrom, also meet all the requirements of 35 U.S.C. ¶ ¶ 1 and 2.

Therefore, It is respectfully requested that all § 112 rejections be reconsidered and withdrawn.

II. CLAIMS 14-16 HAVE BEEN CANCELED IN FAVOR OF THE BROADER CORRESPONDING CLAIMS 27, 37 AND 22, RESPECTIVELY

In the aforementioned Office Action, the Examiner concentrated his discussion on claim 14 and then extended such discussion as applicable to the other independent claims. Because claim 14 has been canceled, the discussion will focus on claims 27-29, which contain similar recitations as canceled claim 14. The discussion will then extend to other claims.

A focus on claim 27 is appropriate because it is broader in scope than canceled claim 14. Moreover, claim 29, which incorporates the limitations of claims 27 and 28, is similar in scope to canceled claim 14. Likewise, claim 37 is broader in scope than claim 15; and, claim 39, which incorporates claim 38, is similar in scope to claim 15. Also, claim 22 is broader in scope than claim 16; and, claim 24, which incorporates claim 23, is similar in scope to claim 15. For greater clarity, however, the discussion of claims 27-29 or any other claims will make reference to corresponding aspects that the Examiner has addressed.

III. CLAIMS 17-66 ARE NOT ANTICIPATED UNDER 35 U.S.C. § 102 BY RIVEST

The Examiner has rejected claims 14-66 as anticipated under 35 U.S.C. § 102(b) by U.S. Patent No. 4,405,829 to Rivest *et al.* ("Rivest"). The Examiner asserts that Rivest teaches (1) using more than two primes in the modulus and (2) using Chinese Remainder Theorem to speed up encryption including the equations recited in the claims. Applicants respectfully disagree. As demonstrated below Rivest (1) fails to teach three or more distinct random prime numbers as claimed, and (2) does not inherently teach certain equations as claimed. Namely, as demonstrated below, Rivest does not teach each and every element of the claimed invention.

Under the tenets of patent law the standards for establishing anticipation are well established. For anticipation under § 102, the cited reference must teach every aspect of the claimed invention, either explicitly or implicitly. Moreover, a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently, in a single prior art reference. Furthermore, the identical invention must be shown in as complete detail as is contained in the claim. Hence, where even one aspect of the claimed invention is not found in a prior art reference, such reference does not anticipate the claimed invention. In addition, to anticipate, the reference must also enable one of skill in the art to make and use the claimed invention, thus placing the allegedly disclosed matter in the possession of the public.

An analysis of Rivest based on these standards clearly shows that Rivest does not teach each and every aspect of Applicants' claimed invention. The analysis also shows that Rivest does not enable one of skill in the art to make and use the claimed invention. Applicants, therefore, respectfully request that the § 102 rejection be withdrawn for pending claims 17-66.[4]

A. Rivest does not Teach Three or More Distinct Random Prime Numbers

In the Office Action, the Examiner states that Applicants' invention is directed to "using more than two primes in the modulus." The Examiner's statement, however, is not precise and mischaracterizes the invention. First, the claimed invention is generally directed to an encryption system and method and, particularly, to establishing cryptographic communications, digital signature generation, and more. For example, the invention as recited in claim 27, is directed to "[a] method for establishing cryptographic communications."[5] Second, a notable feature of the invention is the use of three or more ***distinct random prime numbers*** in the modulus:

> n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ where k is an integer greater than 2, and $p_1, p_2, \ldots, p_k$ are ***distinct random prime numbers.***

---

4 Claims 67-92 have not been rejected under 35 U.S.C. §102 and are assumed allowable over Rivest.

5 Canceled claim 14, which the Examiner addresses in the Office Action, was similarly directed.

Claim 27 (and canceled claim 14). Applicants' specification clearly discloses the importance of this aspect of the invention by describing its high level of security accompanied by its increased efficiency when compared to prior art systems:

> Instead of $n=p \cdot q$, as is universal in the prior art, the present invention discloses a method and apparatus wherein n is developed from three or more distinct prime numbers; i.e., $n=p_1 \cdot p_2 \cdot \ldots \cdot p_k$, where k is an integer greater than 2 and $p_1, p_2, \ldots p_k$ are sufficiently large ***distinct primes***. Preferably, "sufficiently large primes" are prime numbers that are numbers approximately 150 digits long or larger. ... If, as in the prior art, p and q are each on the order of, say, 150 digits long, then n will be on the order of 300 digits long. However, three primes p_2, p_1, and p_3 employed in accordance with the present invention can each be on the order of 100 digits long and still result in n being 300 digits long. ***Finding and verifying 3 distinct primes, each 100 digits long, requires significantly fewer computational cycles than finding and verifying 2 primes each 150 digits long.***

Specification, pg. 6 (emphasis added). Moreover, other advantages would be apparent to one of skill in the art. *Id.* Accordingly, this aspect of the invention cannot be ignored in an anticipation analysis.

By contrast to the present invention, Rivest fails to teach the use of three or more distinct random prime numbers. Indeed, Rivest teaches that a modulus, n, of three or more prime numbers need not use distinct random prime numbers:

> the [Rivest] invention may use a modulus n which is a product of three or more prime numbers (***not necessarily distinct***).

Rivest, col. 13, lines 29-31 (emphasis added). Notably, it is Applicants' use of three or more distinct random prime numbers that provides its high level of security. To use non-distinct prime numbers as taught by Rivest significantly reduces the security of the encryption system. An example illustrates this point. If three prime numbers are used with two of those prime numbers being equal to each other (i.e. non-distinct prime numbers), the required factorization effectively reduces to the factorization of two distinct prime numbers. Contrastingly, the factorization of three distinct random prime numbers is much more difficult and provides a high level of security as disclosed in Applicants' Specification.

Because Rivest does not teach the use of three or more "distinct random prime numbers," it does not teach each and every aspect of independent claim 27. Hence, Rivest does not anticipate independent claim 27 under 35 U.S.C. § 102. Likewise, Rivest does not anticipate

independent claims 17, 22, 32, 37, 42, 47, 52, 57 and 62 under 35 U.S.C. § 102 because such claims also recite the "distinct random prime numbers". Accordingly, claims 17, 22, 27, 32, 37, 42, 47, 52, 57 and 62 are allowable over Rivest.

In view of this, all the dependent claims 18-21, 23-26, 28-31, 33-36, 38-41, 43-46, 48-52, 53-56, 58-61 and 63-66 are also not anticipated by and are allowable over Rivest.

B. Rivest does not Enable Three or More Distinct Random Prime Numbers

Even assuming *arguendo* that Rivest teaches the use of three or more prime numbers, a *prima facie* case of anticipation cannot be supported by Rivest because it does not disclose to one of skill in the art how to make and use the claimed invention. Rivest still fails to anticipate the claimed invention. To anticipate, Rivest must also enable one of skill in the art to make and use the claimed invention, thus placing the allegedly disclosed matter in the possession of the public.[6] It is a major leap to go from Rivest's passing comment on the use of three or more, not necessarily distinct, prime numbers to Applicants' claimed invention employing three or more distinct random prime numbers with the recited equations.

Indeed, not only does it not exists in isolation, the limitation in the claims of three or more distinct random prime numbers implicates and effects other elements of the claims (See independent claims 17, 22, 27, 32, 37, 42, 47, 52, 57 and 62). For example, elements resulting from the claimed use of three or more distinct random prime numbers include the sub-task equations. As recited in claim 27 and other independent claims, the sub-tasks C_1, C_2,..., C_k follow from the use of three or more distinct random prime number. And the necessary details of how to make and use this aspect of the claimed invention are provided in Applicants' disclosure.

By contrast, Rivest does not reveal to one of skill in the art how to extend the use of three or more prime numbers to the claimed sub-tasks. Namely, Rivest does not enable the use of three or more distinct random prime numbers. Hence, this is another reason why Rivest cannot anticipate independent claims 17, 22, 27, 32, 37, 42, 47, 52, 57 and 62 under 35 U.S.C. § 102.

---

6 See, e.g., *Enzo Biochem, Inc. v. Calgene, Inc.*, 52 USPQ2d 1129 at 1135 (Fed. Cir., 2001).

Moreover, claims that depend on a claim that is not anticipated are themselves not anticipated. Accordingly, all the dependent claims 18-21, 23-26, 28-31, 33-36, 38-41, 43-46, 48-52, 53-56, 58-61 and 63-66 are also not anticipated by Rivest.

C. Rivest does not Inherently Teach Certain Equations as Claimed

In addition to the above, it is important to note that Rivest fails to teach further aspects of the invention. In the aforementioned Office Action, the Examiner asserts that "[t]he particular equations specified in claim 14[7] lines 11-24 and 30-32 ... are ***inherent*** in using Chinese Remainder Theorem for decoding as taught by Rivest." Office Action, pg. 5, ¶ 9a (emphasis added). The Examiner, however, has not and cannot make out a *prima facie* case of anticipation under a theory of inherency.

It is established under the tenets of patent law that an element of a claim can be inherent in a prior art reference, but to show inherency is not a matter of simply asserting it. To establish inherency, the extrinsic evidence must make clear that the missing descriptive matter is ***necessarily present*** in the thing described in the reference, although inherency ***may not be established by probabilities or possibilities.*** The mere fact that a certain thing may result form a given set of circumstances is not sufficient. The law is clear that in relying on a theory of inherency, the Examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art. Accordingly, it is well settled that the burden of establishing a *prima facie* case of anticipation under an inherency theory is on the Examiner. Here, the Examiner has not properly supported an inherency theory thus the § 102 rejection cannot stand.

The inherency theory proposed by the Examiner fails because the Examiner's conclusion about particular equations of Applicants' claims being "inherent in using Chinese Remainder Theorem for decoding as taught by Rivest" is not supported and is in contravention of the standards for establishing inherency as set out by the court.[8] Stated another way, the Examiner

---

[7] Because claim 14 has been canceled, Applicants will discuss claims 27-29.

[8] See, e.g., *EMI Group North America, Inc. v. Cypress Semiconductor Corp.*, 60 USPQ2d 1423 at 1429 (Fed. Cir., 2001). Also, for the purposes of the following discussion note that the first set of equations to which the Examiner refers are recited in claim 27 and the second set of equations are recited in claim 29 which depends on claims 27 and 28.

established a starting point, Chinese Remainder Theorem, and then asserted a conclusion that Applicants' claimed equations are inherent in Chinese Remainder Theorem. What the Examiner has not provided is a path based on facts and/or technical reasoning leading from the starting point to the conclusion. Namely, the Examiner did not lay out a path from the citation in Rivest about the "Chinese Remainder Theorem for decoding" to the first set of equations as recited in claim 27, nor did the Examiner lay out a path that leads to the second set of equations as recited in claims 28 and 29.

The passing comment Rivest made regarding Chinese remaindering in a decoding context is as follows:

> ***Decoding*** may be performed modulo each of the prime factors of n and the results combined using "Chinese remaindering" or any equivalent method to obtain the result modulo n.

Rivest, col 13:31-34. From this comment, Inherency does not follow either with regards to these equations or as to encoding. Actually, application of Rivest's comment regarding "Chinese Remainder Theorem for decoding" to claims addressing encoding is a misapplication of Rivest (and misuse of hindsight).[9] Indeed, by contrast to Rivest an element of claim 27, as well as claims 32, 47 and 52, involves "encoding a plaintext message word M to a ciphertext word C." Accordingly Rivest's passing comment cannot, without more, support a *prima facie* case of anticipation under an inherency theory.

A further point is made that inherency is not shown even if it is probable or possible to use Chinese Remainder Theorem in the manner claimed. The law is clear about the insufficiency to support inherency assertion of the mere fact that a certain thing ***may result*** from a given set of circumstances. Here, the Examiner must demonstrate that the claimed equations are ***necessarily present*** in the Chinese Remainder Theorem. Applicants have clearly disclosed that it is possible, indeed desirable, to extend the teachings of Chinese Remainder Theorem in a particular manner, as recited in the claims, for use in a cryptographic method and system. That it is possible, however, does not suffice to meet the Examiner's burden.

---

[9] *See*, e.g., *Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.*, 230 U.S.P.Q. 416 (Fed. Cir. 1986).

Applicants take full notice that the Examiner possesses the authority to require Applicants to prove that the subject matter shown to be in the prior art does not possess the characteristic relied on. However, it is well settled that the Examiner cannot place this burden on Applicants until the Examiner has first set our a *prima facie* case of anticipation based on a theory of inherency. Because the Examiner has not made out a *prima facie* case based on an inherency theory, it is another reason why the rejection of claim 27, and likewise of all the other independent claims 17, 22, 32, 37, 42, 47, 52, 57 and 62, under 35 U.S.C. §102 cannot stand.

It like manner, a claim depending on a claim that is not anticipated is itself not anticipated. Thus, all the dependent claims, claims 18-21, 23-26, 28-31, 33-36, 38-41, 43-46, 48-52, 53-56, 58-61 and 63-66 are also not anticipated by Rivest based on inherency.

D. Rivest does not Enable Certain Equations as Claimed

It is further noted that not only does Rivest fail to support a claim of anticipation based on inherency, it also fails to enable one of ordinary skill in the art how to make and use the claimed equations as recited in claim 17, 22, 27, 32, 37, 42, 47, 52, 57 and 62, and their respective dependent claims. Even assuming *arguendo* that Rivest teaches three or more prime numbers, Rivest does not extend this teaching to the way in which one of ordinary skill in the art might make and use the claimed equations that follow from the use of three or more distinct random prime numbers (as recited in claim 27 and other independent claims, for example, the sub-tasks $C_1, C_2, \ldots, C_k$ follow from the use of three or more distinct random prime number). Accordingly, this is another reason for finding that Rivest does not anticipate independent claims independent claims 17, 22, 27, 32, 37, 42, 47, 52, 57 and 62, and their respective dependent claims 18-21, 23-26, 28-31, 33-36, 38-41, 43-46, 48-52, 53-56, 58-61 and 63-66 under 35 U.S.C. § 102.

E. Conclusion: All the Pending Claims are Patenatble over Rivest

In view of the foregoing discussion Rivest does not teach or suggest each and every element of the claimed invention, nor are the aforementioned elements inherent in the Rivest. In other words, Rivest does not support the foregoing claim rejections under 35 U.S.C. § 102. As all the pending claims 17-66 and 73-92 are allowable over Rivest, Applicants respectfully request that the § 102 rejection of claims 17-66 be withdrawn.

IV. CLAIMS 17-66 AND 73-92 ARE NOT RENDERED OBVIOUS UNDER 35 U.S.C. § 103(A) BY ANY COMBINATIONS OF THE CITED REFERENCES

In addition to the §102 rejections, claims 67-92 have been rejected by the Examiner under 35 U.S.C. §103(a) as being unpatentable over Rivest in view of Menezes et al. ("Menezes") § 14.8. The Examiner has also rejected claims 14-92 under 35 U.S.C. §103(a) as being unpatentable over Menezes, in view of Quisquater, *et al.* ("Quisquater"). It is noted with regard to this rejection that the Examiner used various additional portions of Menezes in conjunction with Quisquater. Hence, as understood by Applicants, the Examiner relies on Menezes § 8.2 in view of Menezes § 3.2 further in view of Quisquater further in view of Menezes § 2.4.3 further in view of Menezes § 14.5.2. It is respectfully submitted that, for reasons as set forth below, the cited references do not support the claim rejections under 35 U.S.C. §103(a).[10]

A. The Cited References are Improperly Combined

For example, in citing Menezes the examiner supplies a clear showing with respect to claim 67 (and, by analogy, to claims 73, 75, 77, 79, 81, 83, 85, 87, 89, and 91) that although Menezes discloses *exponentiation algorithms* (Note at 14.87, pg. 617) it does not disclose the claimed "*exponantiation **units** operating substantially **simultaneously***". Albeit the deficiencies of Rivest as outlined above, the Examiner thus proposes to combine Menezes with Rivest in order to produce the claimed invention since, as the Examiner contends,

> "it would have been obvious to one of ordinary skill in the art [*at the time the invention was made*] to use this method in the invention of Rivest at al. because of Menezes et al's suggestion that efficient exponentiation is essential to employing the RSA algorithm"

However, the tenets of patent law require that, when applying 35 U.S.C. 103, the references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention. Considering the foregoing assertions, however, the Examiner has not shown any support in the prior art for the proposed combination referred to above; nor has the Examiner produced any proof of knowledge in the art suggesting such combined teaching to produce the claimed invention.

---

[10] Because claim 14 has been canceled, Applicants discussion will focus on the corresponding claim elements as recited in claims 27-28.

Namely, obviousness cannot be predicated on what is not known at the time the invention was made. And, in order to establish a *prima facie* case of obviousness, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available in the art, to modify or combine teachings of the references and there must be a reasonable expectation of success. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the cited prior art, and not based on Applicant's disclosure. In this case, the foregoing criteria for *prima facie* showing of making the combination in order to establish obviousness were not met.

1. The Proposed Combination of Rivest and Menezes is Improper

For example, as mentioned, efficiency could be a plausible motivation for using Rivest's RSA encryption in combination with Menzes' *plurality of exponentiation algorithms* (Note at 14.87, pg. 617). However, efficiency is by no means a motivation suggested in the references for producing the claimed "*exponantiation **units** operating substantially **simultaneously***" by combining Rivest's RSA encryption with Menzes' *plurality of exponentiation algorithm*it. Hence, the proposed combination of teachings of the cited references, Menezes and Rivest, in order to produce the claimed invention is entirely improper without the presence of any suggestion or motivation to do so in either of them.

2. Menezes § 8.2 in view of Menezes § 3.2 further in view of Quisquater further in view of Menezes § 2.4.3 further in view of Menezes § 14.5.2 Cannot be Combined

The Examiner additionally asserts that various portions of Menezes in conjunction with Quisquater may be properly combined. As understood by Applicants, the Examiner asserts that Menezes § 8.2 in view of Menezes § 3.2 further in view of Quisquater further in view of Menezes § 2.4.3 further in view of Menezes § 14.5.2 may be combined to render claim 27, and by analogy claims 17-46, obvious under § 103(a). With this combination of references and upon making an assertion of official notice, the Examiner also asserts that claims 47-66 and 73-92 are

rendered obvious. Applying the same standards for considering a proposed combination of references as highlighted above, Applicants respectfully disagree.[11]

a. Menezes § 8.2 Cannot be Properly Combined with Menezes § 3.2

In order to understand why Menezes § 8.2 cannot be properly combined with Menezes § 3.2 it is important to consider the state of the art at the time the invention was made. To that end, is it also important to address the premise proposed by the Examiner regarding Menezes. The Examiner admits that Menezes § 8.2 "lacks a teaching that there can be more than two primes in the modulus.[12]" Office Action, pg. 9, ¶ 12(a)(v). Upon making certain statements about the content of Menezes § 3.2, the Examiner makes the imprecise statement that "[t]he security of the RSA system (Section 8.2) is in fact equivalent to the integer factorization problem, see section 8.2.2(I) (sic) and Fact 8.6." Office Action, pg. 9, ¶ 12(a)(v)(1). Based on this premise, the Examiner concludes that

> "[i]t would be obvious for one of ordinary skill in the art to modify the system of Section 8.2 to have a modulus having the number of primes, 'k,' being a number greater than 2 because the difficulty of the integer factorization problem provides the security for the cryptosystem."

Because his premise is incorrect, the Examiner's conclusion is also incorrect.

A careful review of Menezes § 8.2 reveals the errors in the Examiner's statement. In particular, § 8.2.2(i) does not make reference to the integer factorization problem but rather the RSA problem (RSAP). ("This is called the ***RSA problem*** (RSAP), which was introduced in § 3.3. There is no efficient algorithm known for this problem." (Emphasis in original.)). Menezes § 3.3 states in fact that "[t]he intractability of the ***RSA problem*** forms the basis for the security of the RSA public-key encrypton scheme (§ 8.2) and the RSA signature scheme (§ 11.3.1)." (Emphasis added.) In this manner, Menezes closely intertwines § § 3.3 and 8.2. And, it is important to note that in addressing the RSA problem Menezes § 3.3 discusses the factoring of a positive integer "n that is the product of two primes p and q, but it does not refer back in this

---

[11] Because claim 14 has been canceled, Applicants discussion will focus on corresponding claim elements recited in claims 27-28.

[12] The Examiner's statement mischaracterizes Applicants' claimed invention. This issue will be addressed *infra*.

discussion to the general integer factorization problem. Thus, the RSA problem is in fact not equivalent to the integer factorization problem.

Referring now to the Examiner's mention that Menzes' "lacks a teaching that there can be more than two primes in the modulus."[13] Again, Menezes § 8.2, makes a distinct reference to the RSA problem and in this particular reference it states that:

> [t]he problem of computing the RSA decryption exponent d from the public key (n, e), and the problem of factoring n, are computationally equivalent. When generating RSA keys, ***it is imperative that the primes p and q be selected in such a way that factoring n = pq is computationally infeasible***; see Note 8.8 for more details.

Menezes § 8.2, Fact 8.6. This statement emphasizes factoring a modulus *n* that is the product of *only two* primes, p and q. For completeness, a thorough review of Note 8.8 reveals that its discussion focuses on the selection of *only two* prime numbers, p and q. Indeed, applicants could not find in the "Handbook of Applied Cryptography" by Menezes, et al., any discussion of RSA that involve more than two prime numbers p and q.

This is not surprising since at the time of publication of this book, RSA encryption was well standardized. See, e.g., *PKCS #1 v1.5: RSA Encryption Standard*, RSA Laboratories , at §§ 6-9 (Revised November 1, 1993), which is attached herewith for the Examiner's convenience. The standard in existence at the time the invention was made, defines a modulus n that is the product of *only two* prime numbers, p and q.

This is the environment in which Applicants' claimed invention was made, and against the state of the art in this environment the invention should be considered. Turning back the clock to the time the invention was made, one of ordinary skill in the art in this environment understood that the security of the RSA system relies on the intractability of the factorization of a modulus n that is the product of ***only two*** prime numbers, p and q, *not two or more* as suggested by the Examiner.

It is interesting to further note that even at a time concurrent with the original filing date of the Application (October 26, 1998) the standard then existing defined the modulus n as the

---

[13] Office Action, pg. 9, ¶ 12(a)(v) referring to Menezes § 8.2. Also, See note 12 above.

product of *only two* primes, p and q. See, *PKCS #1 v2.0: RSA Cryptography Standard*, RSA Laboratories (October 1, 1998), which is enclosed herewith for the Examiner's convenience.

Given this background, there is a clear prohibition on gleaning knowledge from Applicants' own disclosure in proposing the combination. Namely, the knowledge attributed to the prior art cannot come from the applicant's invention itself. Applicants' disclosure clearly teaches a security system that is distinguished from RSA cryptography, particularly as it relates to using three or more distinct random prime numbers in Applicants' claimed invention. Applicants discuss several of the advantages of using three or more distinct random prime numbers. Indeed, even if the Examiner, upon reading Applicants' disclosure, wholeheartedly believes that one of skill in the art could have made the claimed invention, such is not the proper inquiry. It is easy to say, "I could have done that," but the point is that, at the time of the Applicants' invention, no one was so inspired. Milton, in his *Paradise Lost,* articulate this point well:

> The invention all admired, and each how he To be the inventor missed; so easy it seemed, Once found, which yet unfound most would have thought, Impossible!

Paradise Lost, Part IV, L. 478-501; *as quoted in, Gillete Co. v. S.C. Johnson & Son, Inc.*, 16 U.S.P.Q.2d 1923 (Fed. Cir. 1990). Of course, many things seem simple when properly taught. Hence, a proper methodology should be followed, especially "in cases where the very ease with which the invention can be understood may prompt one 'to fall victim to the insidious effect of a hindsight syndrome wherein that which only the invention taught is used against its teacher." *In re Kotzab*, 54 U.S.P.Q.2d 1308 (Fed. Cir. 2000).

In the case at hand, Applicants disclose how a cryptographic system using three or more distinct random prime numbers may be used. The mere fact that Applicants' invention relies on known mathematical principles does not alone render the claimed invention obvious to produce by combining the references. The inquiry does not end with one skilled in the art having knowledge of the *RSA problem* and of the *integer factorization problem*. The inquiry must further ask whether a person of ordinary skill in the art would have been motivated to combine this knowledge in order to produce the claimed invention. Here, the art cited by the Examiner does not support the Examiner's proposed combination of Menezes § 8.2 with Menezes § 3.2.

That the RSA problem was strictly confined to producing a modulus, n, that is the product of two prime numbers, in fact, teaches away from Applicants' claimed invention. The standards and teachings of RSA were so entrenched in the use of only two prime numbers, p and q, that one of skill in the are would have been discouraged to follow the path Applicants took. Essentially, there is no suggestion to combine if a reference teaches away from its combination with another source. Teaching away is the antithesis of the art's suggesting that the person of ordinary skill go in the claimed direction. Because Menezes § 8.2 taught away from Applicants' invention, Menezes § 8.2 cannot be properly combined with Menezes § 3.2.

b. Menezes Cannot be Properly Combined with Quisquater

Quisquater deals with an RSA system using a modulus, n, produced from only two primes. Therefore, it is likewise proper to conclude that Quisquater cannot be properly combined with Menezes § 3.2.

B. The Claimed Invention Requires a Combination of Elements that are Entirely absent from the Cited References

Lastly, even if the cited references were properly combined, the claimed invention as recited in the above-enumerated claims requires a combination of elements that are entirely absent from Menezes, singly or in combination with either Rivest or Quisquater. And it is well established that the cited prior art, considered as a whole, must teach or suggest all the claim limitations.

1. Singly or in Combination Rivest in view of Menezes § 14.8 does not Teach or Suggest Each and Every Element of the Claimed Invention

First, the Examiner rejected dependent claims 67-92 as obvious over Rivest in view of Menezes *et al.* ("Menezes"). The Examiner applied Rivest as discussed above in further view of Menezes § 14.8. Note that claims 67-72 have been canceled such that Applicants will address dependent claims 73-92.

Importantly, the Examiner does not assert that that Menezes § 14.8 teaches or suggests the aforementioned "*exponantiation **units** operating substantially **simultaneously***" aspect of now canceled claim 67 (and by analogy claims 73, 75, 77, 79, 81, 83, 85, 87, 89, and 91). Indeed, because Menezes § 14.8 is provided only to address the exponentiation of dependent claims 73-

92 and other similar claims, Menezes § 14.8 cannot provide for the deficiencies of Rivest as discussed *supra*. Thus, Rivest in view of Menezes § 14.8 does not teach or suggest every element of independent claims 67.

Similarly, because of the deficiencies of Rivest as pointed in the discussion *supra*[14], Menezes (notwithstanding it own deficiencies) does not provide for the deficiencies of Rivest with respect to claims 17, 22, 27, 32, 37, 42, 47, 52, 57 and 62. Namely, As demonstrated by the discussion above, Rivest in view of Menezes § 14.8 does not teach or suggest each and every element of the independent claims 17, 22, 27, 32, 37, 42, 47, 52, 57 and 62, and, again, their respective dependent claims 73-92.

2. *Singly or in Combination, Menezes § 8.2 in view of Menezes § 3.2 further in view of Quisquater further in view of Menezes § 2.4.3 further in view of Menezes § 14.5.2 do to not Teach or Suggest Every Element of the Claimed Invention*

At pages 8-9, ¶ ¶ 12(a)(i)-(iv) of the Office Action, the Examiner cites Menezes § 8.2 as teaching certain aspects of Applicants claim 14, but then admits that § 8.2 does not teach certain other aspects.[15] The Examiner admits that Menezes § 8.2 does not teach:

> [(1)] that there can be more than two primes in the modulus,
> [(2)] that the quantities of lines 10-24 of claim [27] are computed,
> [(3)] that the data is (re)combined as in [the equations of claims 28 and 29].

Office Action, pg. 9, ¶ 12(a)(v). Note that the Examiner made a fourth assertion which is obviated by the amendments to the claims and addressed *supra*. To make up for the deficiencies, the Examiner proposes a combination of Menezes § 8.2, Menezes § 3.2, Quisquater, Menezes § 2.4.3 and Menezes § 14.5.2. The following discussion rebuts these assertions.

a. Menezes § 3.2 does not Teach or Suggest Three or More Distinct Random Prime Numbers

The Examiner cites Menezes § 8.2 for the proposition "that there can be more than two primes in the modulus." Office Action, pg. 10, ¶ 12(a)(v). As an initial matter, it is worth correcting the Examiner's misstatement and believed misconception of the claimed inevntion as

---

[14] See discussion above traversing the claim rejections over Rivest of the claims under §102.

[15] Because claim 14 has been canceled, Applicants will discuss claims 27-29.

recited for example in claim 27. Applicants' claim 27 recites that n is a product of *three or more distinct random prime numbers*, specifically:

> n is a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ where k is an integer ***greater than 2*** and $p_1, p_2, \ldots, p_k$ are ***distinct random prime numbers.***

Claim 27 (emphasis added). And, Menezes § 8.2 does not teach or suggests the use of three or more distinct random prime numbers as claimed by Applicants.

The Examiner cites Menezes § 3.2 as teaching that the integer factorization problem comes from factoring *n* the product of multiple primes $p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$. The Examiner then states that

> "[i]t would be obvious for one of ordinary skill in the art to modify the system of Section 8.2 to have a modulus having the number of primes, 'k', being a number greater than 2 because the difficulty of the integer factorization problem provides security for the cryptosystem."

With the comment on "k," the Examiner addresses his stated concern "that there can be more than two primes in the modulus." By considering only that "there can be more than two primes in the modulus," the Examiner has reduced claim 27 down to an "idea" that the Examiner appears to regard as the invention. Distilling an invention down to the "gist" or "thrust" of an invention disregards the requirement of analyzing the subject matter as a whole. Indeed, the Examiner's analysis is not complete. In a complete analysis, according to Menzes § 3.2, the exponents e_1, e_2, ..., e_k are each >1 (for i=o...k, $e_i \geq 1$) and "the p_i are pairwise distinct primes." From $e_i \geq 1$ it follows that in factoring *n* the product of $p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$ each of the primes cannot be distinct and random. It is, therefore, clear that $e_i \geq 1$ does not meet the limitation in claim 27 that "distinct random prime numbers" be used. Ignoring this element of claim 27 is a failure to consider all the claim limitations and a failure of the obviousness analysis.

Applicants take note of the Examiner's comment referring to the "next two paragraphs." Office Action, pg. 10 ¶ 12(a)(v)(1). Applicants have reviewed the next two paragraphs and do not find that the Examiner has addressed distinct random prime numbers as recited in claim 27. Moreover, Applicants have reviewed the rest of the Office Action and, likewise, do not find that the Examiner has addressed this aspect of the claimed invention. Accordingly, Menezes § 3.2

does not teach the use of three or more distinct random prime numbers as recited in independent claim 14 and all other independent claims 15-17, 22, 27, 32, 37, 42, 47, 52, 57 and 62.

b. Quisquater does not Teach or Suggest the Claimed Sub-Task Elements

The Examiner cites Quisquater for the proposition that the "quantities of lines 10-24 [of claim 27[16]] are computed." Office Action, pg. 10, ¶ 12(a)(v)(2). Here again, however, the Examiner has failed to show that the cited reference teaches or suggests an element of the claims. Thus, the Examiner has failed to meet his burden in presenting a *prima facie* case of obviousness under § 103.

A comparison of the equations of Applicants' claim 27 and Quisquater reveals all that Quisquater does not teach. Claim 27 recites detailed equations on how three or more distinct random prime numbers are used in defining three or more sub-tasks in a method for encoding a message (hereafter referred to as "sub-task" elements). Specifically, these "sub-task" elements recite:

defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv M_1^{e_1} \pmod{p_1},$$
$$C_2 \equiv M_2^{e_2} \pmod{p_2},$$
$$\vdots$$
$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$
$$M_2 \equiv M \pmod{p_2},$$
$$\vdots$$
$$M_k \equiv M \pmod{p_k},$$
$$e_1 \equiv e \pmod{(p_1 - 1)},$$
$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$
$$\vdots$$
$$e_k \equiv e \pmod{(p_k - 1)},$$

where e is a number relatively prime to (p_1-1), (p_2-1), ..., (p_k-1).

Claim 27. The details and breadth of these equations are not disclosed by Quisquater.

---

[16] Because claim 14 has been canceled, Applicants discussion will focus on the corresponding claim element recited in claims 27.

Quisquater teaches certain equations applicable to decryption in an RSA-type system employing the product $r = p \cdot q$ and a random integer e that is relatively prime with p-1 and q-1. Quisquater, pg. 906, col. 1. In this context, Quisquater presents the following equations for the residues of the quantities m, c and d:

$$c_1 \equiv c \pmod{p} \qquad c_2 \equiv c \pmod{q}$$
$$d_1 \equiv d \pmod{p-1} \qquad d_1 \equiv d \pmod{q-1}$$
$$m_1 \equiv m \pmod{p} = c_1^{d_1} \pmod{p}$$
$$m_2 \equiv m \pmod{q} = c_2^{d_2} \pmod{q}.$$

Id. Quisquater bases these equations on Chinese Remainder Theorem and applies them to the modulus r. *See*,Quisquater, pg. 906, col. 1. Quisquater, however, discloses equations only in the use of two prime numbers as in classic RSA encryption. Quisquater does not teach or suggest the use of three or more random prime numbers as recited in Applicants' claim 27. It also follows that Quisquater does not teach or suggest the subtask elements of claim 27.

Quisquater relies on the Chinese Remainder Theorem for the proposition that the message, m, can be broken into blocks, m_1 and m_2, for expediting the deciphering process. Quisquater presupposes a two-prime RSA with a modulus, r, with prime factors, p and q. Based on that, it further presupposes that it needs to use a ***maximum length decryption key***, d, for greater security (Quisquater, pg. 906, col. 1), which *teaches away* from the three or more distinct random prime numbers as recited in the claims.

There is no teaching or suggestion anywhere in Quisquater or in other prior art references to extend the teachings of Quisquater to three or more distinct random prime numbers as claimed by Applicant. Thus, there is no teaching of how Quisquater's equations can be applied in a cryptographic scheme employing more than three distinct random prime numbers. Because Quisquater fails in this respect, it does not teach or suggest the sub-task elements of claim 27, singly or in combination with Menezes. By analogy, Quisquater does not teach or suggest the sub-task elements as recited in all the other independent claims 15-17, 22, 27, 32, 37, 42, 47, 52, 57 and 62.

c. Menezes § 2.4.3 does not Teach the Claimed Recursive Combining Process

The Examiner cites Menezes § 2.4.3 for the proposition that it "discloses that the quantities [of claims 28 and 29[17]] are computed." Office Action, pg. 10, ¶ 12(a)(v)(3). The Examiner, however, has failed to show that any elements of claims 28 and 29 are taught or suggested by Menezes § 2.4.3.

Claim 28 recites "performing a recursive combining process to produce said ciphertext word C" (hereafter referred to as the "recursive combining process" element). In the Office Action, the Examiner comments that he accounts for the "recursive" aspect of claim 28 by noting that computers usually compute sums in a recursive manner. The Examiner, however, need not go so far afield. In examining a claim, the Examiner must consider the claim as a whole and in light of the specification while giving due consideration to each and every element of the claim. Here, there is no need to go beyond the claim or the specification to understand the "recursive" aspect of claim 28. As is commonly known by one of ordinary skill in the computational arts, a *recursive expression is an expression, each term of which is determined by application of a formula to preceding terms*. The Specification is consistent with this common understanding when it recites "it has been found that [the sub-tasks, M_1, M_2 and M_3] can most expeditiously be combined by a form of the Chinese Remainder Theorem (CRT) using, preferably, a recursive scheme." Specification pg. 10. The Specification then goes on to give a specific example of a recursive equation:

$$Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n.$$

Specification, pg. 11. The recursive aspect of Y_i is clear: the quantity, Y_i, is determined from preceding terms, Y_{i-1}. Accordingly, this is an example of a recursive combining process as recited in claim 28. In fact, it is exactly the recursive equation recited in claim 29.

With a complete understanding of the recursive combing process at issue, the misapplication of Menezes § 2.4.3 is better understood. Menezes discloses that a solution x to certain simultaneous congruences in the Chinese Remainder Theorem may be computed as

---

[17] Because claim 14 has been canceled, Applicants discussion will focus on the corresponding claim element recited in claims 28 and 29.

$$x = \sum_{i=1}^{k} a_i N_i M_i$$
$$= \sum_{i=1}^{k} a_i N_i (N_i^{-1} \bmod n_i)$$
where
$N_i = n / n_i$, and
$M_i = N_i \bmod n_i$.

Menezes § 2.4.3. This is not a recursive equation. Moreover, this does not teach the recursive combining process term of claims 28 or 29.

In Menezes § 2.4.3, it is clear that the computed quantity x does not depend on previous values of x. Moreover, each quantity a_i, N_i and M_i does not depend on any of their respective previous values. Thus, there is no recursive aspect to Menezes' equation. The Examiner makes some correspondences between the equation of Menezes § 2.4.3, however, these correspondences in no way transform Menezes equation to the recursive combining process of claim 28. The Examiner suggests the following:

> Applicants' w_i corresponds to Menezes N_i;
> Applicants' n corresponds to Menezes n; and
> Applicants' Y_i corresponds to Menezes partial sums of x.

Before applying the Examiner's suggestion, let us first expand the equation in Menezes:

$$x = \sum_{i=1}^{k} a_i N_i M_i$$
$$= \sum_{i=1}^{k} a_i N_i (N_i^{-1} \bmod n_i)$$
$$= a_1 N_1 (N_1^{-1} \bmod n_1) + a_2 N_2 (N_2^{-1} \bmod n_2) + \ldots + a_k N_k (N_k^{-1} \bmod n_k)$$
$$= x_1 + x_2 + \ldots + x_k.$$

Now, applying the Examiner's suggestions, we obtain:

$$Y = \sum_{i=1}^{k} a_i w_i (w_i^{-1} \bmod n_i)$$
$$= a_1 w_1 (w_i^{-1} \bmod n_1) + a_2 w_2 (w_2^{-1} \bmod n_2) + \ldots + a_k w_k (w_k^{-1} \bmod n_k)$$
$$= Y_1 + Y_2 + \ldots + Y_k.$$

Again, this is not a recursive equation and it certainly does not teach or suggest the recursive combining process term of claim 28 or the recursive equation of claim 29. Instead, the equation in Menezes is a straightforward summation that does not teach any aspect of dependent claims

28 or 29. Because claims 18, 23, 33, 38, 43, 47, 53, 58 and 63 are similar to claim 28 and because claims 19, 24, 34, 39, 44, 48, 54, 59 and 64 are similar to claim 29, Menezes § 2.4.3 does not teach or suggest any aspect of these claims either. Accordingly, Menezes § 2.4.3 does not teach or suggest the recursive combining process term as recited in dependent claims 18, 19, 23, 24, 33, 34, 38, 39, 43, 44, 47, 48, 53, 54, 58, 59, 63 and 64.

d. Examiner's Discussion of Menezes § 14.5.2 Cannot Support a *Prima Facie* Case of Obviousness

The Examiner next cites Garner's Algorithm as disclosed in Menezes § 14.5.2. The Examiner, however, does not explain which aspect of any claim he is addressing. From the Office Action, Applicants infer that Garner's Algorithm as discussed in ¶ 12(a)(v)(3)(b) is presented so as to address claims other than claim 27 or 28. *See*, Office Action, pg. 10, ¶ 12(a)(v)(3) ("The subsequent claims are each directed to one of these two algorithms. The algorithms are Gauss' Algorithm which is detailed in [12(a)(v)(3)](a) and Garner's Algorithm, which is detailed in [12(a)(v)(3)](b).") Although the Examiner states that "[t]he following are some correspondences for the reader's convenience," he does not present any correspondences at all. *See*, Office Action, pg. 11, ¶ 12(a)(v)(3)(b). This is unfortunate because some correspondences would have shed light onto which claims the Examiner was addressing. The Examiner comments that Garner's Algorithm is recursive, but because the Examiner seems to be addressing an equation other than the recursive equation discussed *supra*, this comment does not elucidate the Examiner's analysis because there are no other recursive equations in any of the claims other than the one discussed *supra*.

Because the Examiner's arguments at ¶ 12(a)(v)(3)(b) are incoherent, they cannot serve as the basis for a *prima facie* case that the claimed invention is obvious.

e. Menezes § 8.2 in view of Menezes § 3.2 further in view of Quisquater further in view of Menezes § 2.4.3 further in view of Menezes § 14.5.2 does not Teach or Suggest Each and Every Element of the Claimed Invention

In the discussion above, Applicants pointed out the deficiencies of the cited references. Whereas the individual references are deficient in certain respects, the combination of references does not provide for the deficiencies the individual references.

As discussed, *supra*, Menezes § 3.2 does not teach or suggest three or more distinct random prime numbers. Applicants have reviewed Menezes § § 2.4.3, 8.2 and 14.5.2 as well as Quisquater and find that none of these references address, much less teach or suggest, the use of three or more distinct random prime numbers.

As discussed, *supra*, Quisquater does not teach or suggest the claimed sub-tasks. Applicants have reviewed Menezes § § 3.2, 2.4.3, 8.2 and 14.5.2 and find that none of these references address, much less teach or suggest, the claimed sub-task elements.

As discussed, *supra*, Menezes § 2.4.3 does not teach or suggest the claimed recursive combining process. Applicants have reviewed Menezes § § 3.2, 8.2 and 14.5.2 as well as Quisquater and find that none of these references address, much less teach or suggest, the claimed recursive combining process.

Thus, Menezes § 8.2 in view of Menezes § 3.2 further in view of Quisquater further in view of Menezes 2.4.3 further in view of Menezes § 14.5.2 does not teach or suggest every element of the independent claim 27. For similar reasons, this combination of references does not teach or suggest every element of the other independent claims, 17, 22, 32, 37, 42, 47, 52, 57 and 62.

C. Conclusion: All Pending Claims are Patentable over the cited References Singly or Combined

The combination of Menezes § 8.2 in view Menezes § 3.2 further in view of Quisquater further in view of Menezes § 2.4.3 further in view of Menezes § 14.5.2 does not teach or suggest, e.g.,:

(1) the use of three or more distinct random prime numbers as claimed;

(2) the claimed sub-task elements; and

(3) the claimed recursive combining process.

Thus, the Examiner has not shown a *prima facie* case of obviousness.

Because the cited references, either singly or in combination, do not teach or suggest every element of independent claim 27, it cannot be rendered obvious under 35 U.S.C. § 103.

For similar reasons, all the other independent claims 17, 22, 32, 37, 42, 47, 52, 57 and 62 are not rendered obvious by the cited references.

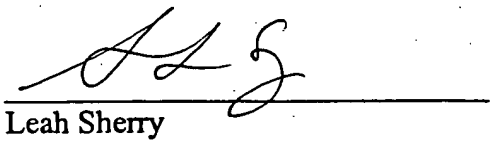
It is axiomatic that claims that depend on a non-obvious claim are themselves non-obvious. Accordingly, all the dependent claims 18-21, 23-26, 28-31, 33-36, 38-41, 43-46, 48-52, 53-56, 58-61 and 63-66 and 73-92 are non-obvious.

In other words, claims 17-66 and 73-92 are allowable over he cited references. Applicants, therefore, respectfully request that the § 103 rejection be withdrawn for all pending claims 17-66 and 73-92.

V. CONCLUSION

In view of the foregoing amendments and remarks, it is submitted that the application is in condition for allowance and a notice of allowance of the pending claims 17-66 and 73-92 is respectfully requested. In the event that a telephone conference would expedite prosecution of the application, the Examiner is respectfully invited to contact the undersigned by telephone at the number set out below.

Respectfully submitted,



Leah Sherry
Reg. No. 43,918

Dated: November 30, 2001
OPPENHEIMER WOLFF & DONNELLY LLP
Customer No. 25696
P.O. Box 10356
Palo Alto, Ca 94303

APPENDIX A:

VERSION WITH MARKINGS TO SHOW CHANGES MADE

17. (Three Times Amended) A method for establishing cryptographic communications ~~that are backwards compatible with preexisting public key transformation schemes~~, comprising the steps of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$$0 \leq M \leq n-1,$$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, C is a number representative of an encoded form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C, whereby

$$C \equiv M^e \pmod{n},$$

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

decoding said ciphertext word C to a receive message word M', said decoding step being performed using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1) \ldots (p_k-1)),$$

said decoding step including the further steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M', wherein M'=M.

22. (Three Times Amended) A cyptographic communications system for establishing communications ~~that are backwards compatible with preexisting public key transformation schemes~~, comprising:

a communication medium;

encoding means coupled to said communication medium and adapted for transforming a transmit message word M to a ciphertext word C and for transmitting said ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$, wherein n is a composite number of the form,

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$

wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein said ciphertext word C corresponds to a number representative of an enciphered form of said message and corresponds to

$C \equiv M^e \pmod{n}$,

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

decoding means communicatively coupled with said communication medium for receiving said ciphertext word C via said medium, said decoding means being operative to perform a decryption process for transforming said ciphertext word C to a receive message word

M', wherein M' corresponds to a number representative of a deciphered form of C, said decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1)\ldots(p_k-1)),$$

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)},$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M' whereby M'=M.

27. (Three Times Amended) A method for establishing cryptographic communications ~~that are backwards compatible with preexisting public key transformation schemes~~, comprising the step of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, wherein said step of encoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$e_k \equiv e \pmod{(p_k - 1)},$$

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results $C_1, C_2, \ldots C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

32. (Three Times Amended) A cyptographic communications system for establishing communications ~~that are backwards compatible with preexisting public key transformation schemes~~, comprising:

a communication medium;

encoding means coupled to said communication medium and operative to transform a transmit message word M to a ciphertext word C, and to transmit said ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$, are distinct random prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, said encoding means being operative to transform said transmit message word M to said ciphertext word C by performing an encoding process comprising the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$e_k \equiv e \pmod{(p_k - 1)},$$

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results $C_1, C_2, \ldots C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

37. (Three Times Amended) A method for establishing cryptographic communications ~~that are backwards compatible with preexisting public key transformation schemes~~, comprising the steps of:

decoding a ciphertext word C to a message word M, wherein M corresponds to a number representative of a message and wherein

$0 \leq M \leq n-1$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, C is a number representative of an encoded form of message word M that is encoded by transforming said message word M to said ciphertext word C whereby

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1);

said decoding step being performed using a decryption exponent d that is defined by

$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1) \ldots (p_k-1))$,

wherein said step of decoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$$M_1 \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2 \equiv C_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv C_k^{d_k} \pmod{p_k},$$

wherein

$C_1 \equiv C \pmod{p_1}$,

$C_2 \equiv C \pmod{p_2}$,

$\vdots$

$C_k \equiv C \pmod{p_k}$,

$d_1 \equiv d \pmod{(p_1 - 1)}$,

$d_2 \equiv d \pmod{(p_2 - 1)}$, and

$\vdots$

$d_k \equiv d \pmod{(p_k - 1)}$,

solving said sub-tasks to determine results $M_1, M_2, \ldots M_k$, and

combining said results of said sub-tasks to produce said message word M.

42. (Three Times Amended) A cyptographic communications system for establishing communications ~~that are backwards compatible with preexisting public key transformation schemes~~, comprising:

a communication medium;

decoding means communicatively coupled with said communication medium for receiving a ciphertext word C via said medium, and being operative to transform said ciphertext word C to a receive message word M', wherein a message M corresponds to a number representative of a message and wherein,

$0 \leq M \leq n-1$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein said ciphertext word C is a number representative of an encoded form of said message word M that is encoded by transforming M to said ciphertext word C whereby,

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1);

said decoding means being operative to perform a decryption process using a decryption exponent d that is defined by

$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1) \ldots (p_k-1))$,

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with,

$M_1' \equiv C_1^{d_1} \pmod{p_1}$,

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein,

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M', whereby M'=M.

47. (Three Times Amended) A method for generating a digital signature ~~that is backwards compatible with preexisting public key transformation schemes~~, comprising the step of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of message word M, wherein

$C \equiv M^d \pmod{n}$, and

wherein said step of signing includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{d_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

wherein d is defined by

$$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1)), \text{ and}$$

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results C_1, C_2, ... C_k, and

combining said results of said sub-tasks to produce said ciphertext word C.

52. (Three Times Amended) A digital signature generation system ~~that is backwards compatible with preexisting public key transformation schemes~~, comprising:

a communication medium;

digital signature generating means coupled to said communication medium and operative to transform a transmit message word M to a signed ciphertext word C, and to transmit said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$, are distinct random prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of said message word M, wherein

$C \equiv M^d \pmod{n}$,

said digital signature generating means being operative to transform said transmit message word M to said signed ciphertext word C by performing a digital signature generating process comprising the steps of,

defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{d_k} \pmod{p_k},$$

where,

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

wherein d is defined by,

$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1),

solving said sub-tasks to determine results $C_1, C_2, \ldots C_k$, and

combining said results of said sub-tasks to produce said signed ciphertext word C.

57. (Three Times Amended) A digital signature process ~~that is backwards compatible with preexisting public key transformation schemes~~, comprising the steps of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$$0 \leq M \leq n-1$$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, C is a number representative of a signed form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C whereby,

$$C \equiv M^d \pmod{n},$$

wherein d is defined by

$$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1)), \text{ and}$$

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

verifying said ciphertext word C to a receive message word M' by performing the steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{e_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$e_1 \equiv e \pmod{(p_1 - 1)}$,

$e_2 \equiv e \pmod{(p_2 - 1)}$, and

$\vdots$

$e_k \equiv e \pmod{(p_k - 1)}$,

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M', whereby M'=M.

62. (Three Times Amended) A digital signature system ~~that is backwards compatible with preexisting public key transformation schemes~~, comprising:

a communication medium;

digital signature generating means coupled to said communication medium and adapted for transforming a message word M to a signed ciphertext word C and for transmitting said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$, wherein n is a composite number of the form

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$,

wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein said signed ciphertext word C corresponds to a number representative of a signed form of said message word M and corresponds to

$C \equiv M^d \pmod{n}$,

wherein d is defined by

$d \equiv e^{-1} \bmod ((p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

digital signature verification means communicatively coupled with said communication medium for receiving said signed ciphertext word C via said medium, and being operative to verify said signed ciphertext word C by performing the steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{e_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

$$e_2 \equiv e \pmod{(p_2 - 1)},$$

$$\vdots$$

$$e_k \equiv e \pmod{(p_k - 1)},$$

solving said sub-tasks to determine results M_1', M_2', ... M_k', and

combining said results of said sub-tasks to produce said receive message word M' wherein M'=M.